

**UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF CALIFORNIA**

UNITED STATES OF AMERICA,

v.

RUDY ESPUDO et al.,

Defendants.

CASE NO. 12-CR-236 - IEG

**ORDER DENYING DEFENDANT
GRADO'S MOTION TO
SUPPRESS CELL SITE AND
SIMULATED CELL SITE
EVIDENCE**

[Doc. No. 1002]

Presently before the Court is the motion of Defendant Miguel Grado ("Defendant" or "Defendant Grado") to suppress cell site and simulated cell site evidence. [Doc. No. 1002, Def.'s Mot.] For the following reasons, the Court **DENIES** the motion.

BACKGROUND

This case involves charges of conspiracy, racketeering, illegal drug distribution, extortion, and money laundering in connection with the Mexican Mafia prison gang and several affiliated Sureno street gangs operating in northern San Diego county. Defendant Grado filed the present motion to suppress on April 8, 2013. [Id.] Defendant Grado seeks to suppress cell site and simulated cell site evidence which he believes was obtained by the Government in violation of Title III of the Electronic Communications Privacy Act of 1986 ("ECPA") and the Fourth

1 Amendment. [Id. at 1-2.] The Government filed a response in opposition to the
 2 motion on May 3, 2013. [Doc. No. 1033.] Defendant Rudy Espudo (“Defendant
 3 Espudo”) subsequently filed a reply memorandum. [Doc. No. 1056, Def.’s Reply.]

4 On April 30, 2013, Defendant Grado had a change of plea hearing before
 5 Magistrate Judge Skomal, where all pending motions were withdrawn as to
 6 Defendant Grado only. [Doc. No. 1024.] On May 23, 2013, Defendant Espudo had
 7 a change of plea hearing before this Court, where all pending motions were
 8 withdrawn. [Doc. No. 1083.] At oral argument on May 16, 2013, the Court deemed
 9 all parties joined in Defendant Grado’s motion. [Doc. No. 1061.] Accordingly, the
 10 present motion remains pending as to the remaining Defendants.

11 DISCUSSION

12 The Fourth Amendment protects the “right of people to be secure in their
 13 persons, houses, papers, and effects, against unreasonable searches and seizures.”
 14 U.S. Const. amend. IV. In order to invoke the protections of the Fourth
 15 Amendment, an individual must have “a justifiable, a reasonable, or a legitimate
 16 expectation of privacy that has been invaded by government action.” Smith v.
 17 Maryland, 442 U.S. 735, 740 (1979) (internal quotation marks omitted).

18 Federal Rule of Criminal Procedure 41 “is the codified expression of Fourth
 19 Amendment law.” In re App. of U.S. for an Order Authorizing Disclosure of
 20 Location Info. of a Specified Wireless Tel., 849 F. Supp. 2d 526, 566 (D. Md. 2011)
 21 (hereinafter “2011 D. Md. Application”). Rule 41 states: “After receiving an
 22 affidavit or other information, a magistrate judge . . . must issue the warrant if there
 23 is *probable cause* to search for and seize a person or property . . .” Fed. R. Crim.
 24 P. 41(d)(1) (emphasis added). Rule 41 provides a general default procedure that
 25 governs searches and seizures, but it “does not modify any statute regulating search
 26 or seizure . . .” Fed. R. Crim. P. 41(a)(1); 2011 D. Md. Application, 849 F. Supp.
 27 2d at 566.

28 ECPA outlines an elaborate statutory scheme which governs electronic

1 surveillance. Pub. L. No. 99-508, 100 Stat. 1848 (1986). ECPA addresses various
2 areas of electronic surveillance including wire taps, tracking devices, stored wire
3 and electronic communications, transactional records, pen registers, and trap and
4 trace devices. Id.; see also 2011 D. Md. Application, 849 F. Supp. 2d at 571. The
5 Court discusses the relevant portions of ECPA below.

6 A portion of Title I of ECPA concerns mobile tracking devices which may
7 move across district lines. Pub. L. No. 99-508, Title I, § 108(a), 100 Stat. 1858
8 (Oct. 21, 1986) (codified at 18 U.S.C. § 3117); 18 U.S.C. § 3117(a). Title I of
9 ECPA defines the term tracking device as “an electronic or mechanical device
10 which permits the tracking of the movement of a person or object.” 18 U.S.C. §
11 3117(b); see also In re App. for Pen Register and Trap/Trace Device with Cell-site
12 Location Authority, 396 F. Supp. 2d 747, 751-52 (S.D. Tex. 2005) (hereinafter
13 “2005 S.D. Tex. Application”). The government must obtain a probable cause
14 warrant under Federal Rule of Criminal Procedure 41 to install and use a mobile
15 tracking device. See United States v. Karo, 468 U.S. 705, 720 (1984); 2005 S.D.
16 Tex. Application, 396 F. Supp. 2d at 751-52.

17 The Stored Communications Act (“SCA”), Title II of ECPA, covers the
18 government’s requests for access to stored records. The SCA permits a
19 governmental entity to “require a provider of electronic communication service or
20 remote computing service to disclose a record or other information pertaining to a
21 subscriber to or a customer of such service (not including the contents of
22 communications) only when the governmental entity . . . obtains a court order for
23 such disclosure.” 18 U.S.C. § 2703(c)(1)(B). The SCA mandates that a court order
24 may only issue “if the governmental entity offers *specific and articulable facts*
25 showing that there are reasonable grounds to believe that the contents of a wire or
26 electronic communication, or the *records or other information sought, are relevant*
27 *and material to an ongoing criminal investigation.*” 18 U.S.C. § 2703(d) (emphasis
28 added). This “specific and articulable facts” standard is a significantly lower legal

1 hurdle than probable cause. See In re App. of the U.S. Directing a Provider of Elec.
 2 Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d 304, 313-315 (3d Cir.
 3 2010).

4 Title III of ECPA covers pen registers and trap and trace devices. Pub. L. No.
 5 99-508, 100 Stat. 1848, 1873 (1986) (codified as amended at 18 U.S.C. §§ 3121-27)
 6 (“Pen/Trap Statute). A pen register is “a device or process which records or
 7 decodes dialing, routing, addressing, or signaling information transmitted by an
 8 instrument or facility from which a wire or electronic communication is transmitted
 9” 18 U.S.C. § 3127(3). A trap and trace device is “a device or process which
 10 captures the incoming electronic or other impulses which identify the originating
 11 number or other dialing, routing, addressing, and signaling information reasonably
 12 likely to identify the source of a wire or electronic communication.” 18 U.S.C. §
 13 3127(4). To install a pen register or trap and trace device, the government only
 14 needs to certify “that the *information likely to be obtained* [from a pen register] is
 15 *relevant to an ongoing criminal investigation*” being conducted by a law
 16 enforcement agency. 18 U.S.C. § 3122(b) (emphasis added). This standard is also
 17 significantly lower than probable cause.

18 In 1994, Congress passed the Communications Assistance of Law
 19 Enforcement Act (“CALEA”), which explicitly prohibits service providers from
 20 disclosing the physical location of the subscriber when the government seeks the
 21 information only on the basis of the Pen/Trap Statute. 47 U.S.C. §§ 1001-1002.
 22 Section 1002 provides, in relevant part, as follows:

23 a telecommunications carrier shall ensure that its equipment, facilities, or
 24 services that provide a customer or subscriber with the ability to originate,
 terminate, or direct communications are capable of—

25 . . .

26 (2) expeditiously isolating and enabling the government, pursuant to a
 27 court order or other lawful authorization, to access call-identifying
 information that is reasonably available to the carrier—

28 (A) before, during, or immediately after the transmission of a wire or

1 electronic communication (or at such later time as may be acceptable to
2 the government); and

3 (B) in a manner that allows it to be associated with the communication to
4 which it pertains, *except that, with regard to information acquired solely*
5 *pursuant to the authority for pen registers and trap and trace devices (as*
6 *defined in section 3127 of Title 18), such call-identifying information*
7 *shall not include any information that may disclose the physical location*
8 *of the subscriber (except to the extent that the location may be determined*
9 *from the telephone number) . . .*

10 47 U.S.C. § 1002(a)(2) (emphasis added).

11 **I. Motion to Suppress Cell Site Location Data**

12 Defendants' argue that the cell site location data acquired by the Government
13 in the present case must be suppressed because it was obtained in violation of Title
14 III of ECPA and the Fourth Amendment. Defendant Grado first argues that the
15 Government was required to obtain a warrant issued on the basis of probable cause
16 before acquiring cell site location data. [*Id.* at 5-7.] Defendant Grado also contends
17 that "[w]hen the government is seeking cell site location information, they are
18 actually seeking tracking device information." [*Id.* at 7.]

19 **A. Scope of the Motion: Historical vs. Real-Time Cell Site Location Data**

20 The Court first addresses whether Defendants' motion pertains to historical
21 and/or real-time cell site location data, as this was initially a matter of some
22 confusion amongst the parties and the Court.

23 Cell site data in the present case refers to the physical location of the single
24 primary cell site/sector at call origination and call termination for each incoming
25 and outgoing call. [*See, e.g.*, Doc. No. 1033-1, App. for Pen Register at 8; Doc. No.
26 1033-1, Order for Pen Register at 22-23.] As commonly used, "historical" cell site
27 data refers to the acquisition of cell site data for a period *retrospective* to the date of
28 the order, whereas "prospective" or "real-time" cell site data refers the acquisition

1 of data for a period of time *going forward from* the date of the order.¹ See, e.g., In
 2 re U.S. for an Order Authorizing the Disclosure of Prospective Cell Site
 3 Information, 412 F. Supp. 2d 947, 949 (E.D. Wisc. 2006) (hereinafter “E.D. Wisc.
 4 2006 Application”) aff’d, 06-MISC-004, 2006 WL 2871743 (E.D. Wis. Oct. 6,
 5 2006). In the present case, the Government applied for orders requesting real-time
 6 cell site data pursuant to 18 U.S.C. § 3123 of the Pen/Trap Statute and § 2703(c)
 7 and (d) of the SCA. [See, e.g., Doc. No. 1002-2, App. for Pen Register at 2.] The
 8 Magistrate Judge’s order permitted the Government to acquire “the location of the
 9 single primary cell site/sector (physical address) at call origination and call
 10 termination for each incoming and outgoing call.” [See, e.g., Doc. No. 1002-2,
 11 Order for Pen Register at 9-10.] The Magistrate Judge’s order was valid for a
 12 prospective period of 60 days. [Id. at 11.]

13 The Government’s opposition to Defendant Grado’s motion focuses on its
 14 argument that it is not required to make a showing of probable cause prior to
 15 acquiring historical cell site location data. [Doc. No. 1033, Govt.’s Opp. at 2-7.]
 16 Defendants’ reply brief highlights the fact that the Government’s opposition brief
 17 did not specifically address the portion of the motion seeking to suppress real-time
 18 cell site location data. [Doc. No. 1056, Def.’s Reply.]

19 Although in its opposition to Defendants’ motion, the Government presents
 20 arguments regarding historical cell site data [See, e.g., Doc. No. 1033, Govt.’s Opp.
 21 at 3 (“Precedent . . . overwhelmingly support the position that no search occurs in
 22 the production of historical cell-site records as occurred in this case.”)], the
 23 Government did not actually obtain historical cell site data in this case. In fact, the
 24 Government acknowledged in its response to the Court’s request for supplemental
 25 briefing regarding historical cell site location data [Doc. No. 1154] that it did not
 26

27
 28 ¹ Courts generally use both “prospective” and “real-time” interchangeably to refer to this type
 of data. This Court will use “real-time” except when quoting other cases which use “prospective.”

1 seek and thus did not obtain an order authorizing the acquisition of historical data.
2 [Doc. No. 1160, Govt.'s Supp. Br.] During oral argument, the Government further
3 clarified that it only obtained cell site location for periods of 60-days going forward.
4 The Government also explained that it referred to the location data it obtained as
5 "historical" because it was maintained by the cell phone provider, however briefly,
6 before it was sent to the Government. Despite the Government's arguments to the
7 contrary, the Court will refer to location data for forward-looking periods of time as
8 "prospective" or "real-time," in accordance with the relevant case law. Because the
9 Government only obtained cell site location data for forward-looking periods of
10 time, the Court will proceed on the motion to suppress as it pertains to real-time cell
11 site location data.

12 Using a combination of statutory and Fourth Amendment analysis, the
13 majority of federal courts examining the requirements for the acquisition of real-
14 time cell site location data mandate that the government make a showing of
15 probable cause. See, e.g., In re App. of U.S. for an Order Authorizing Disclosure of
16 Location Information, 849 F. Supp. 2d 526, 539-42 (D. Md. 2011); In re App. of the
17 U.S. for an Order Authorizing the Disclosure of Prospective Cell-site Info., 2006
18 WL 2871743, at *5 (E.D. Wis. Oct. 6, 2006); In re App. of the U.S. for an Order
19 Authorizing the Monitoring of Geolocation and Cell-site Data for a Sprint Spectrum
20 Cell Phone No. ESN, 2006 WL 6217584, at *4 (D.D.C. Aug. 25, 2006); In re App.
21 of the U.S. for an Order (1) Authorizing the Use of a Pen Register and a Trap and
22 Trace Device, 396 F. Supp. 2d 294 (E.D.N.Y. 2005) (hereinafter "2005 E.D.N.Y.
23 Application"); 2005 S.D. Tex. Application, 396 F. Supp. 2d 747. The minority of
24 federal courts permit the government to obtain this information on a showing that is
25 less than probable cause. See, e.g., In re App. of U.S. for an Order for Prospective
26 Cell Site Location Info., 460 F. Supp. 2d 448 (S.D.N.Y. 2006) (hereinafter "2006
27 S.D.N.Y. App."); In Matter of App. of U.S. for an Order, 411 F. Supp. 2d 678
28 (W.D. La. 2006) (hereinafter "2006 W.D. La. Application"); In re App. of the U.S.

1 for an Order for Disclosure of Telecomm. Records and Authorizing the Use of a Pen
 2 Register and Trap and Trace, 405 F. Supp. 2d 435 (S.D.N.Y. 2005) (hereinafter
 3 “2005 S.D.N.Y. Application”).

4 **A. Statutory Analysis**

5 The Government contends that it may obtain cell site location data upon a
 6 showing of “specific and articulable facts” under the SCA. [*Id.* at 2-3.] The
 7 Government argues that the SCA not only applies to historical cell site data, but also
 8 to real-time cell site data, because even real-time cell site data are business records
 9 generated and stored by cell phone companies. [*Id.* at 3.] At oral argument on July
 10 3, 2013, the Government contended that even real-time cell site location data is an
 11 *historical* record, as it is stored and maintained by the cell phone provider before it
 12 sends the data to the Government.

13 **1. Business Records**

14 At oral argument, the Government summarily argued that real-time cell site
 15 location data is a business record because the data is initially transferred to the cell
 16 phone provider, even if only for a few seconds, before being transmitted to the
 17 Government. As a result, the Government contended that there is no cognizable
 18 difference between historical and real-time cell site location data. However, the
 19 issue is not as straightforward as the Government implies.

20 The SCA states that “[a] governmental entity may require a provider of
 21 electronic communication service or remote computing service to disclose a record
 22 or other information pertaining to a subscriber to or customer of such service (not
 23 including the contents of communications)” Although, it does not define the
 24 term “record,” the language of the SCA makes clear that the record must pertain to a
 25 subscriber’s electronic communication service. ECPA, of which the SCA is a part,
 26 defines the term “electronic communication service” as “any service which provides
 27 to users thereof the ability to send or receive wire or electronic communications.”
 28 18 U.S.C. § 2510(15).

Despite that real-time cell site location data may constitute information relating to a subscriber's electronic communication service as defined by ECPA, the Court finds that this data nevertheless does not constitute a record. The Court finds persuasive the Magistrate Judge's reasoning in In re Application for Pen Register and Trap/Trace Device with Cell Site Location Authority, 396 F. Supp. 2d 747 (S.D. Tex. 2005) (hereinafter "2005 S.D. Tex. Application"). The Magistrate Judge analyzed the structural differences between the SCA and other titles of ECPA to determine that real-time cell site location information is not obtainable as a "record" under the SCA. The Court adopts the Magistrate Judge's reasoning in full:

Even more compelling is the structural argument against allowing access to prospective cell site data under the SCA. Unlike other titles of the ECPA, which regulate methods of real-time surveillance, the SCA regulates access to records and communications in storage. As implied by its full title ("Stored Wire and Electronic Communications and Transactional Records Access"), the entire focus of the SCA is to describe the circumstances under which the government can compel disclosure of existing communications and transaction records in the hands of third party service providers. Nothing in the SCA contemplates a new form of ongoing surveillance in which law enforcement uses co-opted service provider facilities.

Unlike wiretap and pen/trap orders, which are inherently prospective in nature, § 2703(d) orders are inherently retrospective. This distinction is most clearly seen in the duration periods which Congress mandated for wiretap and pen/trap orders. Wiretap orders authorize a maximum surveillance period of 30 days, which begins to run no later than 10 days after the order is entered. 18 U.S.C. § 2518(5). Pen/trap orders authorize the installation and use of a pen register for a period "not to exceed sixty days." 18 U.S.C. § 3123(c)(1). By contrast, Congress imposed no duration period whatsoever for § 2703(d) orders. Likewise, Congress expressly provided that both wiretap orders and pen/trap orders may be extended by the court for limited periods of time. 18 U.S.C. §§ 2518(5), 3123(c)(2). There is no similar provision for extending § 2703(d) orders. Pen/trap results are ordinarily required to be furnished to law enforcement "at reasonable intervals during regular business hours for the duration of the order." 18 U.S.C. § 3124(b). The wiretap statute authorizes periodic reports to the court concerning the progress of the surveillance. 18 U.S.C. § 2518(6). Again, nothing resembling such ongoing reporting requirements exists in the SCA.

Another notable omission from § 2703(d) is sealing of court records. Wiretap orders and pen/trap orders are automatically sealed, reflecting the need to keep the ongoing surveillance under wraps. 18 U.S.C. §§ 2518(8)(b), 3123(d)(1). The SCA does not mention sealing. Pen/trap orders must also direct that the service providers not disclose the existence of the order to third parties until otherwise ordered by the court.

18 U.S.C. § 3123(d)(2). Section 2705(b) of the SCA authorizes the court to enter a similar non-disclosure order, but only upon a showing of possible adverse consequences, such as “seriously jeopardizing an investigation or unduly delaying a trial.” 18 U.S.C. § 2705(b)(1)-(5).

Taken together, the presence of these provisions in other titles of the ECPA and their corresponding absence from the SCA cannot simply be dismissed as a coincidence or congressional absent-mindedness. Pen registers and wiretaps are surveillance techniques for monitoring communications yet to occur, requiring prior judicial approval and continuing oversight during coming weeks and months; § 2703(d) permits access to customer transaction records currently in the hands of the service provider, relating to the customer’s past and present use of the service. Like a request for production of documents under Federal Rule of Civil Procedure 34, § 2703(d) contemplates the production of existing records, not documents that may be created at some future date related to some future communication. That is the most obvious explanation why the SCA makes no mention of surveillance periods, extensions, periodic reporting, or sealing. If Congress had not intended the SCA to be retrospective in nature, it would have included the same prospective features it built into the wiretap and pen/trap statutes.

Id. at 760-61; see also 2005 E.D.N.Y Application, 396 F. Supp. 2d at 308-09.

Furthermore, § 2703 only authorizes a court to enter an order to turn over data that exists at the time the order is issued, and not data as it is captured. First, the language of the statute contemplates records that are already in existence through the use of the present tense. It states that a court may issue an order requiring the disclosure of records on the basis of the government’s showing that the requested items “*are* relevant and material to an ongoing investigation.” 2005 E.D.N.Y Application, 396 F. Supp. 2d at 312-13 (citing 18 U.S.C. § 2703(d)). Had Congress intended the government to be able to procure information not yet in existence, it could have used the phrase “are or may be.” 2005 E.D.N.Y Application, 396 F. Supp. 2d at 312-13.

Finally, taking the Government’s argument that real-time cell site location data is an historical record to its logical end would lead to perverse results. For example, real-time acquisition of the contents of conversations could be described as stored in the same way that real-time cell site data is under the Government’s theory. The Government could then try to use § 2703(a), which permits it to acquire the contents of wire or electronic communications that have been in storage for 180

1 days or less under Rule 41, to circumvent the additional requirements of Title III.
2 Id. at 313-14.

3 Accordingly, the Court declines to adopt the Government's theory that real-
4 time cell site location data are business records under the SCA.

5 **2. Hybrid Theory**

6 The "hybrid theory" is one that has been commonly put forth by the
7 government when seeking real-time cell site location data. Although the
8 Government in the present case contended that it obtained this data under the SCA,
9 and did not explicitly mention the hybrid theory, the Court nevertheless considers
10 this theory in an abundance of caution, as the hybrid theory is premised on the
11 authority of the SCA being combined with the Pen/Trap Statute.

12 This theory argues for statutory authority to obtain real-time cell site location
13 data using a combination of the SCA, 18 U.S.C. § 2701 *et seq.*, and the Pen/Trap
14 Statute, 18 U.S.C. § 3121 *et seq.*, to overcome the restrictions of CALEA, 47 U.S.C.
15 1001 *et seq.*. See, e.g., 2006 S.D.N.Y. Application, 460 F. Supp. 2d at 460-61; 2005
16 S.D.N.Y. Application, 405 F. Supp. 2d at 447. The hybrid theory, if adopted by the
17 Court, would also allow the Government to circumvent the retrospective nature of §
18 2703, as described above, as the "forward-looking procedural features" of the
19 Pen/Trap statute would allow location data to be collected prospectively. See 2005
20 E.D.N.Y. Application, 396 F. Supp. 2d at 316. Under this theory, the Government
21 would be able to obtain real-time cell site location data on the SCA's lower showing
22 of specific and articulable facts demonstrating relevance and materiality to an
23 ongoing criminal investigation rather than probable cause.

24 Several courts have addressed this issue of whether a combination of the
25 Pen/Trap Statute and the SCA allow the government to obtain real-time cell site
26 data without a showing of probable cause. Although the scope of the data sought
27
28

differs slightly between the cases,² the legal question before each of those courts, and that before this Court remains the same: whether the Government may obtain real-time location data on the lesser showing of specific and articulable facts demonstrating relevance and materiality to an ongoing criminal investigation in place of a showing of probable cause, using a combination of the Pen/Trap Statute and the SCA.

A significant majority of courts have rejected the hybrid theory and has found that real-time cell site location data is not obtainable on a showing of less than probable cause. See, e.g., In re App. of U.S. for an Order for Prospective Cell Site

² Some cases focus on the scope of the data sought as a factor that differentiates various applications for cell site location data. See, e.g., 2006 W.D. La. Application, 411 F. Supp. 2d 678; 2005 S.D.N.Y. Application, 405 F. Supp. 2d 435.

The degree of precision provided by real-time cell site location data depends on multiple variables related to the type and frequency of such data. With regard to the type of data provided, data from a single tower indicates that a cell phone was within the range “covered” by that tower, providing a location within a diameter varying from many miles in rural or suburban areas to several hundred feet in urban areas. In re Application of U.S. for an Order for Prospective Cell Site Location Info. on a Certain Cellular Tel., 460 F. Supp. 2d 448, 450 (S.D.N.Y. 2006) (hereafter “S.D.N.Y. 2006 Application”). Greater precision can be achieved where data from multiple towers provides the relative signal strength and the angle from which a cell phone signal originates. Timothy Stapleton, The Electronic Communications Privacy Act and Cell Location Data, 73 Brook. L. Rev. 383, 388 (2007). By comparing this data from multiple towers through the mathematical process of multilateration (commonly referred to as triangulation) the phone’s location can be placed within anywhere from a few feet to several blocks. U.S. v. Powell, No. 12-cr-20052, 2013 WL 1876761, at *3 (E.D. Mich. May 3, 2013). Where a cell phone has the capability, even greater precision is achievable by obtaining information from a built-in GPS locator. Id. at 4.

With regard to the frequency of real-time location data points, information may be limited to the initiation or termination of each call sent from or received by a phone, may consist of much more frequent periodic information produced every several seconds by normal functions of a phone whenever it is turned “on,” or may be artificially induced whenever law enforcement sends a signal to the target phone (also referred to as “pinging”). Id. at 3; Stapleton, supra at 389.

For example, 2005 S.D.N.Y. Application distinguishes its situation where it granted the government’s application seeking data only when telephone calls are made and from only one cell tower, with other cases where the government sought more precise triangulated data. Id. at 437-38. In this section, the Court considers the statutory authority for the Government’s acquisition of real-time cell site data in this section, and not constitutional authority. Under the Court’s reasoning, the scope of the data sought does not affect the statutory analysis. See In the Matter of the App. of the U.S. for Orders Authorizing the Installation and Use of Pen Registers and Caller Identification Devices on Tel. Nos. [Sealed] and [Sealed], 416 F. Supp. 2d 390, 392-93, 395 (D. Md. 2006) (hereinafter “2006 D. Md. Application”) (“[T]he fact that the requested information reveals less precise location information does not change the statutory analysis.”).

1 Location Info. on a Certain Cellular Tel., 2006 WL 468300 (S.D.N.Y. Feb. 28,
 2 2006); 2006 D. Md. Application, 416 F. Supp. 2d 390; In re U.S. for an Order
 3 Authorizing Disclosure of Prospective Cell Site Info., 412 F. Supp. 2d 947 (E.D.
 4 Wisc. 2006); In re Apps. of U.S. for Orders Authorizing Disclosures of Cell Cite
 5 [sic] Info., 2005 WL 3658531 (D.D.C. Oct. 26, 2005); 2005 S.D. Tex. Application,
 6 396 F. Supp. 2d 747; 2005 E.D.N.Y. Application, 396 F. Supp. 2d 294. A minority
 7 of courts, on the other hand, have found that it is. See, e.g., 2006 S.D.N.Y.
 8 Application, 460 F. Supp. 2d 448; 2005 S.D.N.Y. Application, 405 F. Supp. 2d 435.

9 Under the Pen/Trap Statute, “pen register” is defined as “a device or process
 10 which records or decodes dialing, routing, addressing, or signaling information
 11 transmitted by an instrument or facility from which a wire or electronic
 12 communication is transmitted” 18 U.S.C. § 3127(3). Absent any other
 13 statutory provisions, cell site data may be obtained pursuant to the Pen/Trap Statute
 14 as this data constitutes signaling information.³ See 2006 E.D. Wisc. Application,
 15 412 F. Supp. 2d at 953; In re U.S. for an Order Authorizing Installation and Use of a
 16 Pen Register, 415 F. Supp. 2d 211, 214 (W.D.N.Y. 2006) (hereinafter “2006
 17 W.D.N.Y. Application”); 2005 S.D.N.Y. Application, 405 F. Supp. 2d at 438-39
 18 (citing U.S. Telecom. Ass’n v. FCC, 227 F.3d 450, 458, 463-64 (D.C. Cir. 2000)
 19 and legislative history); but see 2005 S.D. Tex. Application, 396 F. Supp. 2d at 761.

20 However, CALEA states: “[W]ith regard to information acquired solely
 21 pursuant to the authority for pen registers and trap and trace devices . . . call-
 22 identifying information shall not include any information that may disclose the
 23 physical location of the subscriber” 47 U.S.C. § 1002(a)(2). As cell site
 24 location data would disclose the physical location of a subscriber, CALEA clearly
 25 prohibits the government from obtaining it solely on the authority of the Pen/Trap
 26

27
 28 ³ The term “signaling information” was added by the USA PATRIOT Act in 2001. See Pub.
L. No. 107-56, § 216(c)(2), 115 Stat. 272, 290 (2001).

statute. See United States v. Powell, --- F.Supp.2d ---, 2013 WL 1876761, at *13 (E.D. Mich. May 3, 2013) (“[T]he information sought here is clearly location data and the government therefore cannot acquire it solely on the authority of the pen/trap statute.”); 2005 S.D.N.Y. Application, 405 F. Supp. 2d at 441.

The hybrid theory generally attempts to overcome CALEA’s hurdle by combining the authority of the Pen/Trap Statute with the SCA, as CALEA is not a blanket prohibition on the disclosure of physical location, but only a prohibition on disclosure *solely* pursuant to the Pen/Trap Statute. In 2005 S.D.N.Y. Application, the Magistrate Judge accepted the hybrid theory and concluded that cell site location data could be obtained by use of the SCA in conjunction with the Pen/Trap Statute. 2005 S.D.N.Y. Application, 405 F. Supp. 2d at 449. The Magistrate Judge relied on the language of CALEA, focusing on the words “solely pursuant,” to suggest that such data may be obtainable using the Pen/Trap Statute in combination with another statute. See id.; see also 2006 S.D.N.Y. Application, 460 F. Supp. 2d at 457-58. The Magistrate Judge reasoned that:

[S]ection 2703 [SCA] is the most obvious candidate to be used in combination with the Pen Register Statute to authorize the ongoing collection of cell site information because it covers cell site information generally. Section 2703’s absence of procedural provisions that typically attach to the transmission of ongoing information is explained by the fact that the pen register is the proper ‘device’ to obtain cell-site information. Thus, the Pen Register Statute’s procedural provisions that are tied to such a device are appropriately combined with an application under section 2703 to obtain such information.

Id.

Courts have examined two variants of the hybrid theory. In 2006 S.D.N.Y. Application, the district court endorsed a permutation of the hybrid theory that relied on the finding that real-time cell site location data is a stored, historical record. Id. at 459-60. As this Court has already rejected the Government’s argument that real-time cell site location data is a stored, historical record, the Court rejects the variant of the hybrid theory propounded in 2006 S.D.N.Y. Application.

A second variant of the hybrid theory does not rely on real-time cell site

1 location data being a “record” under the SCA. This variant, addressed by the
 2 Magistrate Judge in 2005 S.D. Tex. Application, 396 F. Supp. 2d 747, is premised
 3 on the argument that cell site data is non-content subscriber information. Id. at 761.
 4 Even assuming that this data constitutes “non-content subscriber information,” the
 5 Court still rejects the hybrid theory for the following reasons.

6 The Court disagrees with the reasoning in 2006 S.D.N.Y. Application that the
 7 word “solely” reflects Congress’s intent to authorize acquisition of real-time cell
 8 site data using this combination of statutes, specifically, the Pen/Trap Statute and
 9 the SCA. See 2006 D.D.C. Application, 2006 WL 41229, at *11 (“I cannot
 10 predicate such a counter-intuitive conclusion on the single word solely.”)

11 The Court begins with the first rule of statutory interpretation which counsels
 12 consulting the express language of the statute. See Williams v. Taylor, 529 U.S.
 13 420, 431 (2000). There is nothing in the relevant statutory language that suggests
 14 that courts may combine the SCA with the Pen/Trap Statute to permit the
 15 acquisition real-time cell site data on a standard lower than probable cause. See
 16 2006 W.D.N.Y. Application, 415 F. Supp. 2d at 214-15 (“[T]here is nothing in the
 17 express language of the Pen Statute, CALEA or ECPA which instructs judges to
 18 follow the particular convergence theory the government suggests.”). The Court
 19 finds the reasoning of the Western District of New York to be persuasive:

20 One would assume that if Congress wanted judges to grant the disclosure
 21 of real time cell site data by importing the procedural rules and safeguards
 22 of a statute that Congress directed not be used to authorize the disclosure
 23 of prospective cell site location data (the Pen Register statute) into a
 24 statute and under a standard that Congress specifically reserved for the
 25 production of historical telephone records (the SCA), Congress could
 26 have and would have clearly said so. Congress did not. “The familiar
 27 ‘easy-to-say-so-if-that-is-what-was-meant’ rule of statutory interpretation
 28 has full force here.” Comm’r of Internal Revenue v. Beck’s Estate, 129
 F.2d 243, 245 (2d Cir.1942).

2006 W.D.N.Y. Application, 415 F. Supp. 2d at 214-15. Despite use of the word
 “solely” in CALEA, the intent to combine the Pen/Trap Statutes with the SCA is not
 at all evidenced by the language of any of the relevant statutes. See 2006 E.D.

1 Wisc. Application, 412 F. Supp. 2d at 958 (“If Congress intended to allow
 2 prospective cell site information to be obtained by means of the combined authority
 3 of the SCA and the Pen/Trap Statute, such intent is not at all apparent from the
 4 statutes themselves.”). Additionally, neither of the statutes used to craft the hybrid
 5 theory explicitly cross-references the other. See 2005 S.D. Tex. Application, 396 F.
 6 Supp. 2d at 764-65 (“The [G]overnment’s hybrid theory, while undeniably creative,
 7 amounts to little more than a retrospective assemblage of disparate statutory parts to
 8 achieve a desired result.”).

9 Because the statutory language is far from clear, the Court consults legislative
 10 history. Heppner v. Alyeska Pipeline Serv. Co., 665 F.2d 686, 871 (9th Cir. 1981)
 11 (“When the meaning of statutory language is unclear, one must look to the
 12 legislative history.”). Courts have inferred from CALEA’s legislative history the
 13 government’s view at the time of the enactment of CALEA that the Pen/Trap Statute
 14 would not be used to secure location information. See, e.g., 2006 E.D. Wisc.
 15 Application, 412 F. Supp. 2d at 955-56; In re Matter of the Application of the
 16 United States of America for an Order Authorizing the Release of Prospective Cell
 17 Site Information, 407 F. Supp. 2d 134, 137-38 (D.D.C. 2006) (hereinafter “2006
 18 D.D.C. Application”).

19 During congressional deliberations on CALEA, in response to the concerns of
 20 “privacy-based” groups over the access of law enforcement to call setup information
 21 which could permit tracking of subscribers, Federal Bureau of Investigation (“FBI”)
 22 Director Louis Freeh (“Director Freeh”) explicitly stated that physical location data
 23 could not be disclosed through the use of a pen register or trap and trace device.

24 Director Freeh stated:

25 The term “call setup information” is essentially the dialing information
 26 associated with any communication which identifies the origin and
 27 destination of a wire or electronic communication obtained through the
 28 use of a pen register or trap and trace device pursuant to court order. *It does not include any information which might disclose the general location of a mobile facility or service, beyond that associated with the area code or exchange of the facility or service. There is no intent*

whatsoever, with reference to this term, to acquire anything that could properly be called "tracking" information. . . .

Law enforcement's requirements set forth in the proposed legislation include an ability to acquire "call setup information." This information relates to dialing type information -- information generated by a caller which identifies the origin, duration, and destination of a wire or electronic communication, the telephone number or similar communication address. Such information is critical to law enforcement and, historically, has been acquired through use of pen register or trap and trace devices pursuant to court order.

Several privacy-based spokespersons have criticized the wording of the definition regarding this long-standing requirement, alleging that the government is seeking a new, pervasive, automated "tracking" capability. Such allegations are completely wrong.

In order to make clear that the acquisition of such information is not being sought through the use of a pen register or trap and trace device, and is not included within the term "call setup information," we are prepared to add a concluding phrase to this definition to explicitly clarify the point: except that such information (call setup information) shall not include any information that may disclose the physical location of a mobile facility or service beyond that associated with the number's area code or exchange.

Statement of Louis J. Freeh, Director, FBI, Before the Senate Judiciary Subcomm. on Tech. and the Law and the Subcomm. on Civil and Constitutional Rights, March 18, 1994, Federal Document Clearing House (hereinafter "Statement of Director Freeh"), at *23, *29, available at 1994 WL 223962 (emphasis added). In fact, the "concluding phrase" that Director Freeh referenced in his statement was codified in CALEA. 47 U.S.C. § 1002(a)(2); see also 2006 D.D.C. Application, 407 F. Supp. 2d at 138.

Furthermore, Director Freeh's statement makes clear that he did not believe CALEA relates to the SCA:

[A]s is clearly set forth in the "purpose" section of the proposed legislation, the intent of the legislation is to maintain existing technical capabilities and to "clarify and define the responsibilities of common carriers . . . to provide the assistance required to ensure that government agencies can implement court orders and lawful authorizations to intercept the content of wire and electronic communications and acquire call setup information under Chapters 119 and 206 of Title 18 and Chapter 36 of Title 50.11.["] These chapters have nothing to do with "transactional information" under our federal electronic surveillance and privacy laws. All telecommunications "transactional" information is already protected by federal law and is exclusively dealt with in Chapter 121 of Title 18 of the United States Code [SCA]. The proposed legislation does not relate

1 to Chapter 121 of Title 18.

2 Statement of Director Freeh, at *27-28 (emphasis added); see also 2005 E.D.N.Y.
 3 Application, 396 F. Supp. 2d at 319-20. “If, as Director Freeh explained, the
 4 proposed legislation did not relate to the SCA, it is exceedingly difficult to adopt the
 5 government’s view that the exception clause specifically authorizes the Court to
 6 apply substantive provisions of the SCA in reviewing [a] cell site application.”
 7 2006 W.D.N.Y. Application, 415 F. Supp. 2d at 217; see also 2006 E.D. Wisc.
 8 Application, 412 F. Supp. 2d at 958 (“In the face of [Director Freeh’s] testimony, it
 9 makes no sense to me that, by the use of the word ‘solely’ in 47 U.S.C. § 1002(a)(2),
 10 Congress was in some back-handed fashion intending to allow the SCA to be used
 11 in conjunction with the Pen/Trap Statute to obtain the very information that Director
 12 Freeh assured Congress he was not seeking the authority to obtain under the
 13 proposed legislation.”).

14 Furthermore, the House Report on CALEA, reaffirmed Director Freeh’s
 15 statements regarding its intent to preclude location information from being obtained
 16 using the authority for pen registers and trap and trace devices:

17 In the eight years since the enactment of ECPA, society’s patterns of
 18 using electronic communications technology have changed dramatically.
 19 . . .

20 Therefore, [CALEA] includes provisions, which FBI Director Freeh
 21 supported in his testimony, that add protections to the exercise of the
 22 government’s current surveillance authority. *Specifically, the bill . . .*
 23 *[e]xpressly provides that the authority for pen registers and trap and*
 24 *trace devices cannot be used to obtain tracking or location information,*
 25 *other than that which can be determined from the phone number.*
 26 *Currently, in some cellular systems, transactional data that could be*
 27 *obtained by a pen register may include location information.*

28 H.R. Rep. 103-827 at 17, reprinted at 1994 U.S.C.C.A.N. 3489, 3497 (Oct. 4, 1994)
 (emphasis added).

Finally, the Court’s rejection of the hybrid theory does not impermissibly read
 the word “solely” out of CALEA. See 2006 S.D.N.Y. App., 460 F. Supp. 2d at 457-
 58 (expressing concern for reading “solely” out of the statutory language of CALEA

1 if the hybrid theory is rejected). The hybrid theory “is not the only way to salvage
 2 independent meaning for CALEA’s use of the word ‘solely.’” 2005 E.D.N.Y.
 3 Application, 396 F. Supp. 2d at 321. As the Magistrate Judge in 2005 E.D.N.Y.
 4 Application notes, the Government could seek an order to install a wiretap on a
 5 mobile phone which concurrently seeks authorization to use a pen register to
 6 acquire cell site location information. Id. The Magistrate Judge concluded that “it
 7 makes perfect sense that Congress would want to allow such usage, realizing that
 8 the showing of probable cause on a number of matters necessary to satisfy the
 9 super-warrant requirements of Title III would satisfy the privacy-based concern that
 10 location information should not be available on a mere certification of relevance.”
 11 Id.

12 In light of Director Freeh’s testimony that location data is not obtainable
 13 under the Pen/Trap Statute and that CALEA did not relate to the SCA, the Court
 14 cannot accept the hybrid theory.

15 Upon review of the statutory scheme, the Court finds that an application for
 16 real-time cell site location data does not implicate any statute regulating search or
 17 seizure or special circumstances. Accordingly, the terms of Rule 41 govern in the
 18 present case. See 2005 E.D.N.Y. Application, 396 F. Supp. 2d at 322 (“I view the
 19 plain language of Rule 41 as providing a default mode of analysis that governs any
 20 matter in which the government seeks judicial authorization to engage in certain
 21 investigative activities.”); see also In re Application of U.S. for an order relating to
 22 Target Phone 2, 733 F. Supp. 2d 939, 943 (N.D. Ill. 2009) (“The government may
 23 obtain real-time cell site information under Federal Rule of Criminal Procedure 41 .
 24 . . on an application supported by probable cause.”). Therefore, a warrant to obtain
 25 real-time cell site location data may only be granted if the Government makes a
 26 showing of probable cause. Fed. R. Crim. P. 41(d).

27 3. Tracking Device

28 In their motion, Defendants also argue that “[w]hen the government is

1 seeking cell site location information, they are actually seeking tracking device
2 information.” [Doc. No. 1002-1, Def.’s Mot. at 7.] The Court need not address this
3 tracking device argument as the Court has already found that a warrant based on
4 probable cause warrant is required to obtain real-time cell site location data.

5 **C. Fourth Amendment**

6 Defendants also argue that the acquisition of cell site location data without a
7 warrant requiring a showing of probable cause violated their Fourth Amendment
8 Rights, and therefore must be suppressed. [Doc. No. 1002-1, Def’s Mot. at 5-6.]
9 Because the Court concludes that statutory authority for obtaining real-time cell site
10 location data on a showing of less than probable cause is lacking, the Court declines
11 to proceed to the Fourth Amendment analysis.

12 **D. Good Faith Exception**

13 Even though the Court finds that Government is required to show probable
14 cause prior to obtaining real-time cell site location data, which it did not do in the
15 present case, the evidence may nevertheless be admissible under the good faith
16 exception.

17 The exclusionary rule was adopted as a “judicially created remedy designed
18 to safeguard Fourth Amendment rights generally through its deterrent effect”
19 United States v. Calandra, 414 U.S. 338, 348 (1974). “Under this rule, evidence
20 obtained in violation of the Fourth Amendment cannot be used in a criminal
21 proceeding against the victim of the illegal search and seizure. . . . This prohibition
22 applies as well to the fruits of the illegally seized evidence.” Id. at 347 (internal
23 citations omitted).

24 Starting from the premise that the exclusionary rule is a judicially created
25 remedy, the Supreme Court created a good faith exception to the application of the
26 exclusionary rule in United States v. Leon, 468 U.S. 897 (1984). Under this
27 exception, the exclusionary rule does not bar “the government’s introduction of
28 evidence obtained by officers acting in objectively reasonable reliance on a search

1 warrant that is subsequently invalidated.” United States v. Luong, 470 F.3d 898,
2 902 (9th Cir. 2006) (citing Leon, 468 U.S. at 918-21). The “good faith test is an
3 objective one.” Luong, 470 F.3d at 902. The Court must ask “whether a reasonably
4 well trained officer would have known that the search was illegal despite the
5 magistrate’s authorization.” Id. (quoting Leon, 468 U.S. at 922 n.23).

6 “[T]he Supreme Court has identified at least four situations in which reliance
7 on a warrant cannot be considered objectively reasonable, and therefore the good
8 faith exception cannot apply: (1) when the affiant knowingly or recklessly misleads
9 the judge with false information; (2) when the judge wholly abandons his or her
10 neutral role; (3) when the affidavit is so lacking in indicia of probable cause that
11 official belief in its existence is objectively unreasonable; and (4) when the warrant
12 is so facially deficient that executing officers cannot reasonably presume it to be
13 valid (i.e. it fails to specify the place to be searched or the things to be seized).”
14 Luong, 470 F.3d at 902 (citing Leon, 468 U.S. at 914, 923).

15 In this case, the Government’s reliance on the SCA and the Magistrate
16 Judges’ orders granting the applications was objectively reasonable. First, the
17 Government’s reliance on the SCA was reasonable. Acts of Congress are entitled to
18 a strong presumption of constitutionality. United States v. Watson, 423 U.S. 411,
19 416 (1976). It was reasonable for the Government to apply for cell site location
20 data under the SCA. There is no clear, controlling case explicitly stating that the
21 government may not obtain real-time cell site location data under the SCA. At
22 most, there are only conflicting district court decisions on the subject. See United
23 States v. Jones, 908 F. Supp. 2d 203, 214-15 (D.D.C. 2012) (stating that “reasonable
24 minds may differ as to whether § 2703 permits law enforcement to seek
25 authorization for prospective cell-site information”).

26 The Government’s reliance on the Magistrate Judges’ orders was also
27 objectively reasonable. The Magistrate Judges approved the Government’s
28 applications. See Leon, 468 U.S. at 921 (“In the ordinary case, an officer cannot be

1 expected to question the magistrate's . . . judgment that the form of the warrant is
 2 technically sufficient. Once the warrant issues, there is literally nothing more the
 3 policeman can do in seeking to comply with the law." (internal quotation omitted)).
 4 Furthermore, the Magistrate Judges applied the correct standard under the SCA and
 5 found that the government "set forth specific and articulable facts showing that
 6 there are reasonable grounds to believe that the subscriber and other information
 7 sought, including cell site location information, is relevant and material to an
 8 ongoing criminal investigation" [Doc. No. 1002, Order for Pen Register at 9.]
 9 See United States v. Graham, 846 F. Supp. 2d 384, 406 (D. Md. 2012); United
 10 States v. Suarez-Blanca, 2008 WL 4200156, at *12 (N.D. Ga. Apr. 21, 2008).

11 Finally, Defendants do not raise any of the exceptions to the good faith
 12 exception. On independent examination of the exceptions, the Court finds that none
 13 of them apply to the present case. Accordingly, even though the Government did
 14 not obtain a warrant based on probable cause prior to seeking real-time cell site
 15 location data, which this Court finds is required, this evidence is nonetheless
 16 admissible under the good faith exception. The Court **DENIES** Defendants' motion
 17 to suppress cell site location data.

18 **III. Motion to Suppress Simulated Cell Site Data**

19 Defendants also seek to suppress simulated cell site evidence. [Doc. No.
 20 1002, Def.'s Mot.] In its opposition brief, the Government requests that the Court
 21 deny the motion to suppress simulated cell site evidence as moot because "no data
 22 from any attempted uses of cell-site simulators were utilized to further the
 23 investigation and no such data will be introduced at trial by the Government."
 24 [Doc. No. 1033, Govt.'s Opp. at 7-8.] In support, the Government cites a
 25 declaration by Special Agent Mathew Zeman who states that "[he is] familiar with
 26 attempts to utilize cell-site simulators" and that "[n]one of these attempts
 27 produced data that was utilized to further the investigation." [Doc. No. 1004-1,
 28 Zeman Decl. at 4, ¶ 7.] Because the Government will not introduce simulated cell


1 site data at trial and because no data from attempted uses of cell-site simulators were
2 used to further the investigation, the Court **DENIES AS MOOT** Defendants'
3 motion to suppress simulated cell site data.

4 **CONCLUSION**

5 In light of the foregoing, the Court **DENIES** Defendants' motion to suppress
6 cell site location data on the basis of the good faith exception. The Court **DENIES**
7 **AS MOOT** Defendants' motion to suppress simulated cell site data.

8 **IT IS SO ORDERED.**

9 **DATED:** July 19, 2013

10 
11 **IRMA E. GONZALEZ**
12 **United States District Judge**